



DOC Code: AP.PRE.REQ

PTO/SB/33 (08-08)

Approved for use through 09/30/2008. OMB 0651-0031

United States Patent & Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

PRE-APPEAL BRIEF REQUEST FOR REVIEWDocket Number (Optional)
059643.00228

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed
Name _____

Application Number:

10/614,343

Filed: July 8, 2003

First Named Inventor:

Gabor BAJKO

Art Unit: 2442

Examiner: John M. MACILWINEN

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

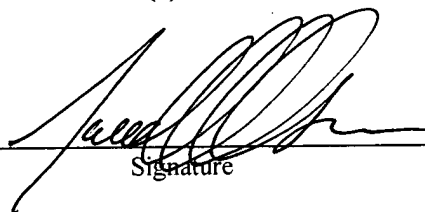
Note: No more than five (5) pages may be provided.

I am the

- ☐ Applicant/Inventor.
- ☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under
37 CFR 3.73(b) is enclosed (Form PTO/SB/96)

☒ Attorney or agent of record.
Registration No. 61,058

☐ Attorney or agent acting under 37 CFR 1.34.
Registration Number if acting under 37 CFR 1.34 _____


SignatureJared T. Olson

Typed or printed name

(703) 720-7800

Telephone number

March 16, 2009

Date

NOTE: Signatures of all of the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Confirmation No.: 7843

Gabor BAJKO

Art Unit: 2442

Application No.: 10/614,343

Examiner: John M. MACILWINEN

Filed: July 8, 2003

Attorney Dkt. No.: 059643.00228

For: A COMMUNICATION SYSTEM

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MAIL STOP: AF

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

March 16, 2009

Sir:

In accordance with the Pre-Appeal Brief Conference Pilot Program guidelines set forth in the July 12, 2005 Official Gazette Notice, Applicant hereby submits this Pre-Appeal Brief Request for Review of the final rejections of claims 1-2, 4-10, 13, 22-25, 46, and 56-71 in the above identified application. Claims 1-2, 4-10, 13, 22-25, 46, and 56-71 were finally rejected in the Office Action dated October 27, 2008. Applicant filed a Response to the final Office Action on January 6, 2009, and the Office issued an Advisory Action dated January 29, 2009, maintaining the final rejections of claims 1-2, 4-10, 13, 22-25, and 56-71. Applicant hereby appeals these rejections and submits this Pre-Appeal Brief Request for Review.

Claims 1-2, 4-10, 22-25, 46 and 56-71 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Jennings and Peterson (RFC 3325 Internet Draft, <http://tools.ietf.org/html/draft-ietf-sip-asserted-identity-00>, May 27, 2002 ("Jennings")) in view of W. Marshall et al. (draft-ietf-sip-privacy-04txt, February 27, 2002 ("Marshall")), and further in view of 3GPP TSG SA WG3 Security – S3#18, Proposed changes to 33.2000 about Za, Zb, Zc interfaces ("3GPP"). While the Office Action took the position that "Jennings...does not show modifying when a message has not been through a security check...[or] wherein the message has been received with security at a first layer," the Office Action also took the position that

Marshall cures these deficiencies of Jennings. Additionally, while the Office Action took the position that “Jennings in view of Marshall do not explicitly show where the message that has been received with security is at a first layer,” the Office Action also took the position that these limitations are disclosed by 3GPP. Applicant respectfully asserts that the Office Action has committed a clear error in presenting this rejection because none of claims 1-2, 4-10, 22-25, 46 and 56-71 are obvious under 35 U.S.C. § 103(a).

Claim 1, upon which claims 2, 4-10, 13, and 63-67 depend, is directed to an apparatus that includes a determiner configured to determine whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer. The apparatus also includes a forwarder configured to forward the message within said first network regardless of the result of the determination. The apparatus further includes a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check when the result of the determination is that the message has not been through a security check, wherein said second layer is a higher layer than said first layer. Independent claims 22, 25, and 46, upon which claims 23-24, 56-62, and 68-71 depend, recite similar limitations, though each has its own scope.

Each of claims 1-2, 4-10, 22-25, 46 and 56-71 recites limitations that are not disclosed or suggested by a combination of Jennings, Marshall, and 3GPP.

Jennings discusses private extensions to session initiation protocol (SIP) that enable a network of trusted SIP servers to assert the identity of end users or end systems, and the application of existing privacy mechanisms. In Jennings, the use of the extensions is only applicable inside an administrative domain with previously agreed-upon policies for generation, transport, and usage of such information.

Marshall discusses extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy. Marshall discloses that the use of these extensions are only applicable inside an administrative domain, or among federations of administrative domains with previously agreed-upon policies for usage of such information.

3GPP discusses proposed changes regarding Za, Zb, and Zc interfaces. The 3GPP document addresses UMTS key management and distribution architectures for native IP based

protocol. The UMTS key management and distribution architecture is based on IPsec IKE protocol.

However, a combination of Jennings, Marshall, and 3GPP fails to disclose or suggest all the limitations of claims 1-2, 4-10, 22-25, 46 and 56-71. For example, a combination of Jennings, Marshall, and 3GPP fails to disclose or suggest “a determiner configured to determine whether a message...has been received with security at a first layer...and a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check when the result of the determination is that the message has not been through a security check,” as recited in claim 1, and as similarly recited in claims 22, 25, and 46.

Instead, Jennings discloses a proxy server in a Trust Domain that receives messages from nodes that it may or may not trust (see Jennings Section 5). On one hand, when a proxy server receives a message from a node it does not trust, the proxy must authenticate the originator of the message, and use the identity which results from this authentication to insert an appropriate P-Asserted-Identity header field into the message. (see Jennings Section 5). On the other hand, if the proxy receives a message from a node that it trusts, the proxy server can use the information in the P-Asserted-Identity header field, if any, as if it had authenticated the user itself. (see Jennings Section 5).

As such, Applicant respectfully asserts that the proxy server in Jennings carries out both the security check and authentication operations at the SIP layer (i.e., at the same layer). Evidence supporting this assertion includes the fact that Jennings is entitled “Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks.” Additionally, the Abstract of Jennings states that “This document describes private extensions to SIP.” Furthermore, section 2 of Jennings states that a trust domain is defined by the reference: Watson, M., “Short term requirements for Network Asserted Identity”, draft-ietf-sipping-nai-reqs-01 (work in progress), May 2002, which states:

We say that node A, in the domain is trusted by a node B, (or B trusts A) if and only if:

- (i) there is a secure connection between the nodes, AND
- (ii) B has *configuration information indicating that A is a member of the Trust Domain* (emphasis added).

As such, Applicant respectfully asserts that Jennings carries out both the security check and the authentication operations at the same layer. Consequently, Applicant respectfully asserts that Jennings fails to disclose or suggest that, for example, a determination about security at a network layer as a basis for including an application layer indication in a message.

Similarly, Applicant respectfully asserts that 3GPP discloses operations that are disclosed on the same layer. For instance, Applicant respectfully asserts that 3GPP teaches applying network layer security at each leg of a route towards a final destination. The bottom paragraph of page 1 of the 3GPP reference states that “All traffic from a NE in one security domain towards a NE in a different security domain will be routed via a SEG and will be afforded hop-by-hop security protection towards the final destination.” As such, the application of security at the IP network layer for one leg of a route results in the application of security at the same IP network layer for a subsequent leg of the route. Consequently, Applicant respectfully asserts that 3GPP fails to disclose or suggest that, for example, a determination about security at a network layer as a basis for including an application layer indication in a message.

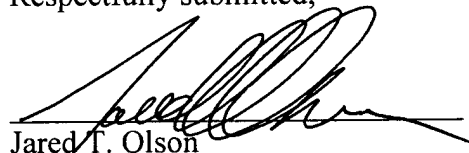
Further, Applicant respectfully submits that Marshall fails to disclose the performing an operation on one layer in response to a determination made on another layer. Rather, Marshall discloses Marshall, when a proxy receives a message from a trusted entity, the proxy does not apply any special processing until the message is forwarded (See Marshall, Section 7.5). However, when the proxy receives a message from an untrusted entity, the proxy MUST examine the message for the presence of any Remote-Party-ID headers (*Id.*). Depending upon the identity of the calling party, the proxy in Marshall performs various operations such as including a calling subscriber Remote-Party-ID in the message or add an rpi-screen parameter set to “no” (*Id.*).

Accordingly, Applicant respectfully asserts that, for example, Marshall fails to disclose or suggest using a determination about security at a network layer as a basis for including an application layer indication in a message.

In light of the above, a combination of Jennings, Marshall, and 3GPP fails to disclose or suggest "a determiner configured to determine whether a message...has been received with security at a first layer...and a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check when the result of the determination is that the message has not been through a security check," as recited in claim 1, and as similarly recited in claims 22, 25, and 46. Accordingly, the Office Action committed a clear error in rejecting claims 1-2, 4-10, 22-25, 46 and 56-71 under 35 U.S.C. § 103(a).

Reconsideration and withdrawal of the rejections, in view of the clear errors in the Office Action, is respectfully requested. In the event this paper is not being timely filed, the Applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Jared T. Olson
Registration No. 61,058

Customer No. 32294

SQUIRE, SANDERS & DEMPSEY LLP

14TH Floor

8000 Towers Crescent Drive

Vienna, Virginia 22182-6212

Telephone: 703-720-7800

Fax: 703-720-7802

JTO:kh

Enclosures: PTO/SB/33 Form
Notice of Appeal
Petition for Extension of Time
Check No. 20592